(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 399 308 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 90108869.0

(51) Int. Cl.5: G06F 11/16, G05B 9/03

(22) Date of filing: 11.05.90

(30) Priority: 23.05.89 US 356546

(43) Date of publication of application: 28.11.90 Bulletin 90/48

(84) Designated Contracting States: DE GB IT

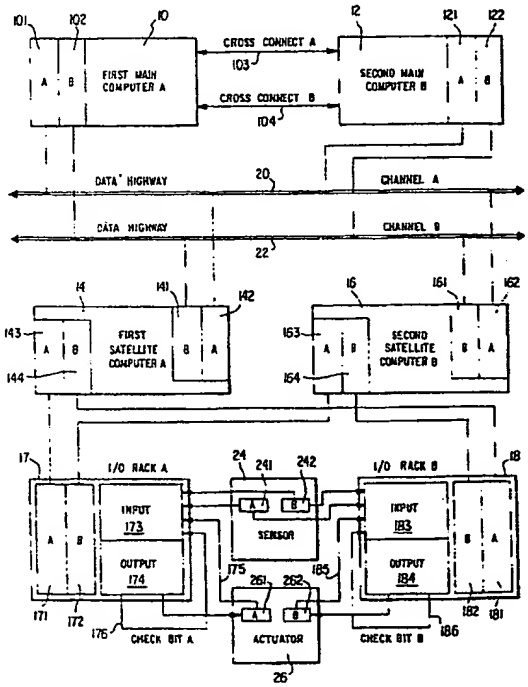
(71) Applicant: AEG WESTINGHOUSE TRANSPORTATION SYSTEMS, INC.
1501 Lebanon Church Road
Pittsburgh, PA 15236-1491(US)

(72) Inventor: Mutone, Gioacchino A.
379 Toura Drive
Pittsburgh, Pennsylvania 15236(US)

(74) Representative: Vogl, Leo, Dipl.-Ing.
AEG Aktiengesellschaft Patente u. Lizenzen
Theodor-Stern-Kai 1 Postfach 70 02 20
D-6000 Frankfurt am Main 70(DE)

(54) Computer network for real time control with automatic fault identification and by-pass.

(57) A computer network for real time control having redundant components for automated fault identification and automated bypass of identified faulty components. The system includes at least two main computers, each coupled to at least two independent parallel data channels. A plurality of satellite computer pairs are connected to these channels, each pair receiving information from a plurality of I/O racks which are connected to redundant sensors for detecting information and to redundant actuators for implementing system control. The main computers are continuously crosslinked and perform evaluation of their respective input and output streams comparing these streams for consistency between the main computers. In the event that an inconsistency is detected in the data streams, the system checks for faulty components to determine the origin of the inconsistency. The system utilizes an evaluation method whereby each main computer independently accesses each of the parallel data channels, satellite computers, I/O racks, sensors and actuators to locate inconsistencies in the data stream. The system then allows for operation with one of the redundant components while the identified defective redundant component is repaired or replaced.



EP 0 399 308 A2

COMPUTER NETWORK FOR REAL TIME CONTROL WITH AUTOMATIC FAULT IDENTIFICATION AND BY PASS

BACKGROUND OF THE INVENTION

The present invention relates to a computer system for performing real time control which has means for identifying faulty components within the computer network. More particularly, the present invention relates to such systems wherein a number of redundant information or data paths are provided to allow for accurate fault identification and to accommodate bypassing faulty components.

Computer systems are commonly utilized to control a wide variety of machinery, performing a wide variety of numerous complex tasks, processes or operations. In order for a computer system to properly accomplish a desired control function, it must rely upon a network to provide the necessary data to perform its controlling function. The network will most commonly consist of a number of sensors for detecting any of the variety of inputs, status or the like and any number of data busses or interfaces for communicating the sensed information to the computer system.

Control information is commonly sent back through the network in response to the sensed information for maintaining proper control of the desired operation. With a complex series of sensors, networks, busses, inputs/outputs and transferring devices, a failure can often arise in such a complex network. Therefore, provisions have to be made to account for errors or failures within the computer system or the information network. Failures must not only be detected and evaluated, but if possible, provisions must be made to circumvent errors or equipment failures in order to allow the system to perform its intended function with the remainder of the network and system in place.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a computer network capable of detecting and analyzing failures and to perform real time control despite the occurrence of such failures.

It is another object of the invention to provide a computer control system operating with a data carrying network which is capable of detecting failures within the network, double checking the existence of such failures and rerouting data or information through the network to circumvent failed portions.

These and further objects are accomplished by the present invention through the provision of a computer system and data transmittal network having redundancy, including two identical main computers each having independent interfaces to redundant data transmission pathways, two identical satellite computers having redundant interfaces to redundant data pathways and having redundant input/outputs for redundantly detecting and cross checking data, wherein the inputs and outputs of each satellite computer are compared to the inputs and outputs of the redundant identical satellite computer and both main computers independently compare the input/output data of each satellite computer at each redundant input and output sensor to check for correspondence.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 is a schematic block diagram of the overall operating configuration of a two computer embodiment of the present invention.

DETAILED DESCRIPTION OF AN EXEMPLARY EMBODIMENT

Figure 1 illustrates a redundant data network of the present invention utilized to perform real time control. Two parallel paths, designated A and B, are provided linking main computers 10 and 12 with sensor 24 and actuator 26. Main computer 10 utilizes data path A as its primary path, and B as a secondary or alternative path. Main computer 12 utilizes data path B as its primary path and path A as a secondary. The two identical main computers 10 and 12 each have independent interfaces 101, 102 and 121, 122, respectively. The primary interface 101 of computer 10, designated A, is connected to the first data highway 20 designated channel A. The primary interface 121 of computer 12, designated B, is connected to the second data highway 22, designated channel B. Each main computer 10, 12 has a secondary interface 102, 122 respectively which is connected to channel B or A respectively.

Satellite computers 14 and 16 are also provided. Each of the satellite computers has an A and B interface, 141, 142 and 161, 162, respectively, attached to the A and B data highways 20 and 22. Each satellite computer is connected to each of two identical input/output racks 17 and 18. First satellite computer 14 has rack interfaces 143 and 144 designated A and B, respectively. Second sat-

ellite computer 16 has rack interfaces 163 and 164, designated A and B, respectively.

These interfaces are interconnected to the first and second input/output (I/O) racks 17 and 18 as illustrated, with the A interfaces connected to I/O rack 17 and the B interfaces connected to I/O rack 18.

In the illustrated embodiment two main and two satellite computers are illustrated. In a computer network employing the present invention there are typically two main computers as illustrated, however, there are a number of satellite computer pairs. Each pair collecting data from sensors feeding those pairs through their I/O racks. Each satellite pair controlling a portion of the system through actuators. Each pair can be located within a few feet or several thousand feet from the main computers depending upon the extent of the data highway network.

As illustrated in Figure 1, a sensor 24 and an actuator 26 are connected to the I/O racks 17 and 18. The sensor 24 along with all the other sensors of the network (not illustrated) gather data information from the process or device being monitored and controlled and feed information to the I/O racks 17 and 18. The actuator receives commands from I/O racks 17 and 18 and acts upon the device or system being controlled.

Sensor 24 is provided with redundant transducers 241 and 242 for supplying sensed information to I/O racks 17 and 18. Each transducer supplies information to both of the I/O racks. The I/O racks 17 and 18 are each provided with an input 173, 183, respectively for receipt of the information from the sensor.

The actuator 26 is provided with redundant transducers 261 and 262 which each receive commands from the output register 174 or 184 of one of the I/O rack 17 and 18, respectively. In this manner, the actuator 26 receives redundant commands, however, only one commands is supplied to each of the redundant transducers 261, 262 of the actuator 26. The actuator 26 acts upon the information only when the commands received by each of the transducers 261 and 262 are in agreement. The command outputs from I/O racks 17 and 18 are looped back from the transducers 261 or 262, to the inputs 173 and 183, respectively, of the same I/O rack on lines 175 or 185, so that they can be monitored as any other input signal. Also, each I/O rack is provided with a means for generating a check bit which is also feed back along line 176 or 186 into the input of the same I/O rack. This check bit is utilized to evaluate error checking in the event of signal discontinuity, as will be explained in greater detail later.

In a normal mode of operation, both sides of a redundant system perform the identical control function by reading inputs from their respective sides of the sensor, performing the required logic calculations, and initiating commands. In this manner the first main A computer 10 works with the first satellite A computer 14 and the first I/O A rack 17 to receive data from sensor 24 and to control actuator 26. Simultaneously, the second main B computer 12, second satellite B computer 16 and second I/O B rack 18 act to receive data from sensor 24 and to control actuator 26 in parallel therewith. Each main computer utilizes the respective sets of interfaces and channels A, B respectively all the way down to the sensors and actuators to perform the respective control function.

The present invention teaches a method that utilizes the configuration illustrated in Figure 1 to achieve fault redundant performance with automatic identification of the faulty component within the network or system. The network also achieves automatic bypassing of the faulty component by utilizing the parallel control channel with confidence.

Main computers 10 and 12 are provided with cross-connected links 103 and 104 for continuous monitoring of the input data received by both main computers to check for agreement of this data. Because the loop back along signal lines 175 and 185 of the output to activator 26 is provided as described above, the monitoring between main computers 10 and 12 can check both the input and output to the sensors and actuators, respectively, of both channels.

An essential element in achieving fault redundant performance is the provision in each of the main computers 10 and 12 of software which provides the following function. When a discrepancy is detected in any of the input data, both main computers 10 and 12 note the discrepancy (assuming both main computers are functioning properly). Main computer 10 if operating properly will undertake the initial corrective and diagnostic actions described below, with subsequent notification to second main computer 12. Main computer 12 will wait for a fixed predetermined amount of time to receive such notification. If notification is not received within that time period, then main computer 12 will assume that main computer 10 is not functioning properly and therefore second main computer 12 will undertake the corrective actions described below.

The following discussion refers to diagnostic and corrective action taken by first main computer 10. If, as described above, second main computer 12 is utilized then it will be understood that corresponding components of the B channel would be utilized where A channel components are referenced. Upon detection of a discrepancy in the input or output data from the cross-connect link, main

computer 10 (or in the alternative second main computer 12) utilizes its own alternate interface 102 to the B channel 22 to read directly the redundant data input on data highway B which would normally be channelled to second main computer 12. If, as a result of this cross-check, the data set on channel B coincides with the data set on channel A, then the second main computer 12 or its linkage to data highway 22, channel B, is presumed defective either in the linking mechanism or in the interface 122. Communication to the other cross-connect link 104, B, is utilized to determine if a fault is in the primary, A, cross-connected channel 103. In either situation, operation can continue with both channels being read by one of the main computers 10 or 12 while the other main computer or the defective cross-connect link is serviced.

If the data from the cross-connect channel indicates that a discrepancy is still present when main computer 10 is reading the data off of both channels A and B, then the problem is located either in the first main computer 10 itself or elsewhere within the system network. In order to determine where the problem exists, the first main computer 10 requests the second main computer 12 to read the redundant set of input data on the A channel. Second main computer 12 reads this data through secondary interface 121 and compares it to the data read from channel B on interface 122. If the data sets coincide, then the system fault is in the first main computer 10. Second main computer 12 will therefore be utilized to continue normal operation utilizing both channels A and B while first main computer 10 is serviced.

If, however, upon evaluation by second main computer B the data sets continue to demonstrate a discrepancy, trouble shooting control is resumed as described below by first main computer 10.

If, the cause of the discrepancy was not found through the procedure outlined above, main computer 10 begins a similar trouble shooting procedure that again utilizes the dual redundancy configuration to determine the location of the problem. However, in this error checking sequence, the next level of the system is evaluated, i.e., the satellite computer level. To accomplish this, both main computers 10 and 12 utilize the same satellite computer, either first satellite computer 14 or second satellite computer 16 to collect the input data. The data thus received by each of the main computers 10 and 12 is compared. Then the other satellite computer is utilized. In this manner, the correct operation of each of the satellite computers 14 and 16 can be determined. As detailed above, this procedure will determine which satellite is defective and operation can continue utilizing the other satellite computer while the defective one is serviced.

In a similar manner, the integrity of I/O racks 17 and 18 can be evaluated, switching between racks and comparing data. The network functions can be maintained while identification of a faulty I/O rack is made, and service to that rack is performed.

Through utilizing the procedure outlined above, and by applying this procedure to each level of the network, the systematic evaluation of network components can be accomplished throughout the entire network until the cause of a data fault is determined in any one of the components of the network, including the main computers, interfaces to the data highway, the satellite computers, interface to the I/O racks, the I/O racks or the sensors or actuators.

The check bit feature provided on each I/O rack connecting the output to the input of the same rack, is utilized at any time a comparison of input data changes from unsatisfactory to satisfactory. The redundancy check bit is utilized to insure that the newly obtained coincidence of input data does not reflect a common failure but instead reflects satisfactory data.

For example, in a situation wherein both main computers 10 and 12 switch to obtaining their data through first satellite computer 14, during an error checking sequence described above, the data requires verification. If the data from each channel passed through satellite computer 14 coincides, it could be the result of a common mode failure within satellite computer 14 that effects both channels A and B. In this case, the check bit on each I/O rack is toggled according to a randomly generated sequence. The reception of an identical sequence on the respective input channel is an indication that the coincidence is not due to a common mode failure.

It will be understood that the above description of the present invention is susceptible to various modifications, changes and adaptations, and the same are intended to be comprehended within the meaning and range of equivalents of the appended claims.

Claims

1. A computer system comprising:
first and second main computers, each computer having a primary data interface and a secondary data interface each interface for sending and receiving system signals;
a first data highway for conveying said system signals, connected to said primary interface of said first main computer and to said secondary interface of said second main computer;
a second data highway for conveying said system signals, connected to said primary interface of said

second main computer and to said secondary interface of said first main computer;
first and second satellite computers for relaying said system signals, each connected to said first and second data highways;
first and second I/O racks, each connected to said first and second satellite computers;
a sensor pair for generating selected system signals, connected to each of said I/O racks, and
an actuator pair for reacting to selected system signals connected to each of said I/O racks.

2. The computer system of claim 1, further comprising:
means for comparing said system signals received by said first main computer with said system signals received by said second main computer, and for detecting discrepancies between said signals.

3. The computer system of Claim 1, said first main computer further comprising means for selectively monitoring either said primary interface or said secondary interface of said first main computer;
said second main computer further comprising means for selectively monitoring either said primary interface or said secondary interface of said second main computer.

4. The computer system of Claim 3, further comprising
means for comparing said system signals received by said first main computer with said system signals received by said second main computer, and for detecting discrepancies between said signals; wherein
said selection means are connected to said comparison means for reacting to a detected discrepancy, configuring said first and second main computers for simultaneous monitoring of a common data highway.

5. The computer system of Claim 1, further comprising:
means for selectively enabling said first satellite computer to relay said system signals to said first and second data highways while selectively disabling said second satellite computer from relaying said system signals.

6. The computer system of Claim 1, further comprising:
means for selectively enabling said second satellite computer to relay said system signals to said first and second data highways while selectively disabling said first satellite computer from relaying said system signals.

7. The computer system of Claim 1, further comprising:
means for establishing a signal path between said sensor pair and said first and second satellite computers via said first I/O rack, while blocking a signal path between said sensor pair and said first and second satellite computers via said second I/O rack.

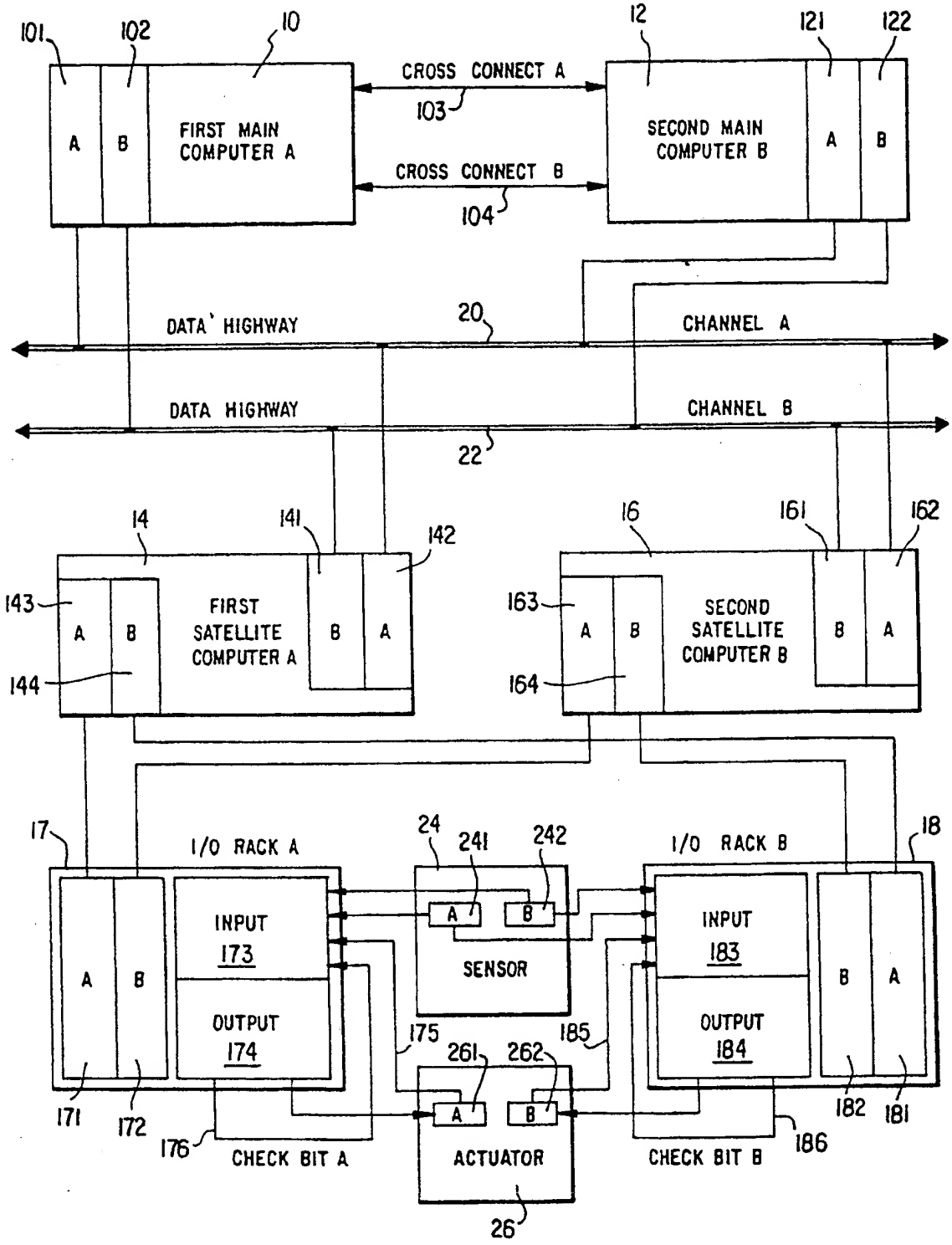
8. The computer system of Claim 1, further comprising:
means for establishing a signal path between said sensor pair and said first and second satellite computers via said second I/O rack, while blocking a signal path between said sensor pair and said first and second satellite computers via said first I/O rack.

9. A method for diagnosis of a computer system according to Claim 2, comprising the steps of:
detecting discrepancies between said system signals received by said first main computer and said system signals received by said second main computer;
monitoring said primary data interface and said secondary data interface of said first main computer and comparing the system signals received thereon for consistency;
utilizing said first satellite computer to relay said system signals between said first I/O rack and said first and second data highways;
utilizing said first I/O rack to establish a data path between said sensor pair and said first and second satellite computers.

Claim 10. A method for monitoring and controlling sensors and actuators, comprising the steps of:
providing first and second main computers;
providing a first signal pathway divided into a plurality of discreet segments, between said main computers and said sensors and actuators;
providing a second signal pathway redundant and parallel to said first signal pathway and having corresponding parallel segments;
selectively monitoring and controlling said sensors and actuators with said first main computer through said first signal pathway;
selectively monitoring and controlling said sensors and actuators with said second main computer through said second signal pathway;
comparing said monitoring by said first computer with said monitoring by said second computer and generating a discrepancy signal in response to the detection a discrepancy between said monitorings during said comparison.

Claim 11. A method according to Claim 10, wherein said step of selectively monitoring with said first computer includes the step of:
selectively bypassing at least one of said segments of said first signal pathway, wherein said corresponding parallel segment of said second signal pathway is substituted therefor.

Claim 12. A method according to Claim 11, wherein said selective bypassing occurs in response to the generation of a discrepancy signal.


101
102
10
12
121
122
A
B
FIRST MAIN COMPUTER A
CROSS CONNECT A
103
CROSS CONNECT B
104
SECOND MAIN COMPUTER B
A
B
DATA HIGHWAY
20
CHANNEL A
DATA HIGHWAY
CHANNEL B
22
14
141
142
16
161
162
143
144
FIRST SATELLITE COMPUTER A
163
164
SECOND SATELLITE COMPUTER B
17
I/O RACK A
24
241
242
I/O RACK B
18
INPUT
173
OUTPUT
174
SENSOR
INPUT
183
OUTPUT
184
175
185
261
262
171
172
176
CHECK BIT A
ACTUATOR
CHECK BIT B
186
182
181
26

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 399 308 A3**

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: **90108869.0**

(51) Int. Cl.5: **G06F 11/16**, G05B 9/03

(22) Date of filing: **11.05.90**

(30) Priority: **23.05.89 US 356546**

(43) Date of publication of application:
28.11.90 Bulletin 90/48

(84) Designated Contracting States:
DE GB IT

(88) Date of deferred publication of the search report:
18.03.92 Bulletin 92/12

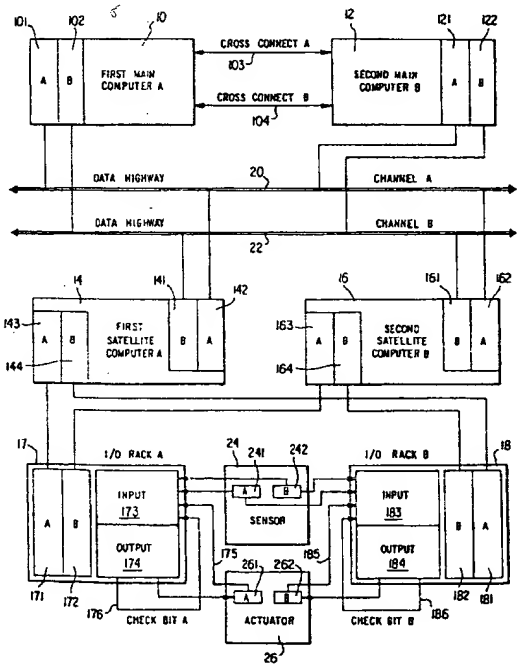
(71) Applicant: **AEG WESTINGHOUSE TRANSPORTATION SYSTEMS, INC.**
1501 Lebanon Church Road
Pittsburgh, PA 15236-1491(US)

(72) Inventor: **Mutone, Gioacchino A.**
379 Toura Drive
Pittsburgh, Pennsylvania 15236(US)

(74) Representative: **Vogl, Leo, Dipl.-Ing.**
AEG Aktiengesellschaft Patente u. Lizenzen
Theodor-Stern-Kai 1 Postfach 70 02 20
W-6000 Frankfurt am Main 70(DE)

(54) **Computer network for real time control with automatic fault identification and by-pass.**

(57) A computer network for real time control having redundant components for automated fault identification and automated bypass of identified faulty components. The system includes at least two main computers, each coupled to at least two independent parallel data channels. A plurality of satellite computer pairs are connected to these channels, each pair receiving information from a plurality of I/O racks which are connected to redundant sensors for detecting information and to redundant actuators for implementing system control. The main computers are continuously cross linked and perform evaluation of their respective input and output streams comparing these streams for consistency between the main computers. In the event that an inconsistency is detected in the data streams, the system checks for faulty components to determine the origin of the inconsistency. The system utilizes an evaluation method whereby each main computer independently accesses each of the parallel data channels, satellite computers, I/O racks, sensors and actuators to locate inconsistencies in the data stream. The system then allows for operation with one of the redundant components while the identified defective redundant component is repaired or replaced.



EP 0 399 308 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number

EP 90 10 8869

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	IEEE MICRO. vol. 7, no. 5, October 1987, NEW YORK US pages 27 - 50; H.D. KIRRMANN ET AL.: 'Fault Tolerance in Process Control: An Overview and Examples of European Products' * page 33, left column, line 1 - page 34, right column, line 23 * *	1	G 06 F 11/16 G 05 B 9/03
A	8TH ANNUAL INTERNATIONAL CONFERENCE ON FAULT-TOLERANT COMPUTING, FTCS-8, JUNE 21-23, 1978 TOULOUSE, FR pages 144 - 149; D.A. RENNELS ET AL.: 'A Study of Standard Building Blocks for the Design of Fault-Tolerant Distributed Computer Systems' * page 148, left column, line 11 - page 149, left column, line 38 * *	1	
A	FR-A-2 561 410 (MERLIN GERIN) * page 1, line 36 - page 3, line 16 * * * page 4, line 17 - page 5, line 12 * * * page 10, line 4 - page 11, line 22 * *	1,2	
A	EP-A-0 229 559 (CIMSA SINTRA) * column 3, line 4 - column 4, line 54 * * * column 6, line 22 - column 7, line 18; figure 1 * *	1	
			TECHNICAL FIELDS SEARCHED (Int. Cl.5) G 06 F G 05 B

The present search report has been drawn up for all claims

Place of search	Date of completion of search	Examiner
The Hague	20 January 92	HERREMAN,G.L.O.

CATEGORY OF CITED DOCUMENTS

X: particularly relevant if taken alone
Y: particularly relevant if combined with another document of the same catagory
A: technological background
O: non-written disclosure
P: intermediate document
T: theory or principle underlying the invention

E: earlier patent document, but published on, or after the filing date
D: document cited in the application
L: document cited for other reasons

&: member of the same patent family, corresponding document